



08-25-00

A

Express Mail No.EL631844520US

Attorney's Docket No. NC13977

Patent

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Box Patent Application
Assistant Commissioner for Patents
Washington, D.C. 20231



NEW APPLICATION TRANSMITTAL

Transmitted herewith for filing is the patent application of

Inventor(s): Scott Probasco

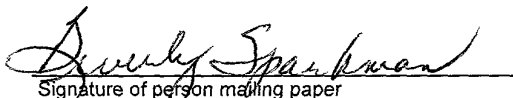
WARNING Patent must be applied for in the name(s) of all of the actual inventor(s) 37 CFR 1.41(a) and 1.53(b)

For (title): KEY DISTRIBUTION FOR ENCRYPTED BROADCAST
DATA USING MINIMAL SYSTEM BANDWIDTH

CERTIFICATION UNDER 37 CFR 1.10

I hereby certify that this New Application Transmittal and the documents referred to as enclosed therein are being deposited with the United States Postal Service on this date, 08/24/2000, in an envelope as "Express Mail Post Office to Addressee" Mailing Label Number EL631844520US, addressed to the: Assistant Commissioner for Patents, Washington, D.C. 20231.

Beverly Sparkman
(type or print name of person mailing paper)


Signature of person mailing paper

NOTE: Each paper or fee referred to as enclosed herein has the number of the "Express Mail" mailing label placed thereon prior to mailing. 37 CFR 1.10(b).

WARNING: Certificate of mailing (first class) or facsimile transmission procedures of 37 CFR 1.8 cannot be used to obtain a date of mailing or transmission for this correspondence.

1. Type of Application

This new application is for a(n)
(check one applicable item below)

☒ Original (nonprovisional)

☐ Design

☐ Plant

WARNING: Do not use this transmittal for a completion in the U.S. of an International Application under 35 U.S.C. 371(c)(4), unless the International Application is being filed as a divisional, continuation or continuation-in-part application

WARNING: Do not use this transmittal for the filing of a provisional application

NOTE: If one of the following 3 items apply, then complete and attach **ADDED PAGES FOR NEW APPLICATION TRANSMITTAL WHERE BENEFIT OF A PRIOR U.S. APPLICATION CLAIMED** and a **NOTIFICATION IN PARENT APPLICATION OF THE FILING OF THIS CONTINUATION APPLICATION**.

☐ Divisional.

☐ Continuation.

☐ Continuation-in-part (C-I-P).

2. Benefit of Prior U.S. Application(s) (35 U.S.C. 119(e), 120, or 121)

NOTE: If the new application being transmitted is a divisional, continuation or a continuation-in-part of a parent case, or where the parent case is an International Application which designated the U.S., or benefit of a prior provisional application is claimed, then check the following item and complete and attach **ADDED PAGES FOR NEW APPLICATION TRANSMITTAL WHERE BENEFIT OF PRIOR U.S. APPLICATION(S) CLAIMED**.

WARNING: If an application claims the benefit of the filing date of an earlier filed application under 35 U.S.C. 120, 121 or 365(c), the 20-year term of that application will be based upon the filing date of the earliest U.S. application that the application makes reference to under 35 U.S.C. 120, 121 or 365(c). [35 U.S.C. 154(a)(2) does not take into account, for the determination of the patent term, any application on which priority is claimed under 35 U.S.C. 119, 365(a) or 365(b).] For a c-i-p application, applicant should review whether any claim in the patent that will issue is supported by an earlier application and, if not, the applicant should consider canceling the reference to the earlier filed application. The term of a patent is not based on a claim-by-claim approach. See Notice of April 14, 1995, 60 Fed. Reg. 20,195, at 20,205

WARNING: When the last day of pendency of a provisional application falls on a Saturday, Sunday, or Federal holiday within the District of Columbia, any nonprovisional application claiming benefit of the provisional application must be filed prior to the Saturday, Sunday, or Federal holiday within the District of Columbia. See 37 C.F.R. § 1.78(a)(3)

☐ The new application being transmitted claims the benefit of prior U.S. application(s). Enclosed are **ADDED PAGES FOR NEW APPLICATION TRANSMITTAL WHERE BENEFIT OF PRIOR U.S. APPLICATION(S) CLAIMED**.

3. Papers Enclosed That Are Required for Filing Date under 37 C.F.R. 1.53(b) (Regular) or 37 C.F.R. 1.153 (Design) Application

 14 Pages of specification

 4 Pages of claims

 1 Page of Abstract

 4 Sheets of drawing

☒ formal

☐ informal

WARNING: *DO NOT submit original drawings. A high quality copy of the drawings should be supplied when filing a patent application. The drawings that are submitted to the Office must be on strong, white, smooth, and non-shiny paper and meet the standards according to § 1.84. If corrections to the drawings are necessary, they should be made to the original drawing and a high-quality copy of the corrected original drawing then submitted to the Office. Only one copy is required or desired. Comments on proposed new 37 CFR 1.84. Notice of March 9, 1988 (1990 O.G. 57-62).*

NOTE "Identifying indicia, if provided, should include the application number or the title of the invention, inventor's name, docket number (if any), and the name and telephone number of a person to call if the Office is unable to match the drawings to the proper application. This information should be placed on the back of each sheet of drawing a minimum distance of 1.5 cm (5/8 inch) down from the top of the page." 37 C.F.R. 1.84(c).

(complete the following, if applicable)

- ☐ The enclosed drawing(s) are photograph(s), and there is also attached a "PETITION TO ACCEPT PHOTOGRAPH(S) AS DRAWING(S)." 37 C.F.R. 1.84(b).

4. Additional papers enclosed

- ☐ Preliminary Amendment
- ☐ Information Disclosure Statement (37 C.F.R. 1.98)
- ☐ Form PTO-1449
- ☐ Citations
- ☐ Declaration of Biological Deposit
- ☐ Submission of "Sequence Listing," computer readable copy and/or amendment pertaining thereto for biotechnology invention containing nucleotide and/or amino acid sequence.
- ☐ Authorization of Attorney(s) to Accept and Follow Instructions from Representative
- ☐ Special Comments
- ☐ Other

5. Declaration or oath

- ☐ Enclosed
- Executed by

(check all applicable boxes)

- ☐ inventor(s).
- ☐ legal representative of inventor(s). 37 CFR 1.42 or 1.43.
- ☐ joint inventor or person showing a proprietary interest on behalf of inventor who refused to sign or cannot be reached.
- ☐ This is the petition required by 37 CFR 1.47 and the statement required by 37 CFR 1.47 is also attached. See item 13 below for fee.

- ☒ Not Enclosed.

WARNING: Where the filing is a completion in the U.S. of an International Application, but where a declaration is not available, or where the completion of the U.S. application contains subject matter in addition to the International Application, the application may be treated as a continuation or continuation-in-part, as the case may be, utilizing ADDED PAGE FOR NEW APPLICATION TRANSMITTAL WHERE BENEFIT OF PRIOR U.S. APPLICATION CLAIMED.

- ☐ Application is made by a person authorized under 37 CFR 1.41(c) on behalf of **all** the above named inventor(s).

[The declaration or oath, along with the surcharge required by 37 CFR 1.16(e) can be filed subsequently.]

NOTE: It is important that all the correct inventor(s) are named for filing under 37 CFR 1.41(c) and 1.53(b).

- ☐ Showing that the filing is authorized.
[not required unless called in question. 37 CFR 1.41(d)]

6. Inventorship Statement

WARNING: If the named inventors are each not the inventors of all the claims an explanation, including the ownership of the various claims at the time the last claimed invention was made, should be submitted.

The inventorship for all the claims in this application are:

- ☐ The same.

or

- ☐ Not the same. An explanation, including the ownership of the various claims at the time the last claimed invention was made,
☐ is submitted.
☐ will be submitted.

7. Language

NOTE: An application including a signed oath or declaration may be filed in a language other than English. A verified English translation of the non-English language application and the processing fee of \$130.00 required by 37 CFR 1.17(k) is required to be filed with the application, or within such time as may be set by the Office. 37 CFR 1.52(d).

NOTE: A non-English oath or declaration in the form provided or approved by the PTO need not be translated. 37 CFR 1.69(b).

- ☒ English
☐ Non-English
☐ The attached translation is a verified translation. 37 CFR 1.52(d).

8. Assignment

- ☐ An assignment of the invention to Nokia Mobile Phones Limited
☐ is attached. A separate ☐ "COVER SHEET FOR ASSIGNMENT (DOCUMENT) ACCOMPANYING NEW PATENT APPLICATION" or ☐ FORM PTO 1595 is also attached.
☒ will follow.

NOTE: "If an assignment is submitted with a new application, send two separate letters—one for the application and one for the assignment." Notice of May 4, 1990 (1114 O.G. 77-78).

WARNING: A newly executed "CERTIFICATE UNDER 37 CFR 3.73(b)" must be filed when a continuation-in-part application is filed by an assignee. Notice of April 30, 1993, 1150 O.G. 62-64.

9. Certified Copy

Certified copy(ies) of application(s)

Country	Appln. no.	Filed
---------	------------	-------

Country	Appln. no.	Filed
---------	------------	-------

Country	Appln. no.	Filed
---------	------------	-------

from which priority is claimed

☐ is (are) attached.

☐ will follow.

NOTE: The foreign application forming the basis for the claim for priority must be referred to in the oath or declaration. 37 CFR 1.55(a) and 1.63.

NOTE: This item is for any foreign priority for which the application being filed directly relates. If any parent U.S. application or International Application from which this application claims benefit under 35 U.S.C. 120 is itself entitled to priority from a prior foreign application, then complete item 18 on the ADDED PAGES FOR NEW APPLICATION TRANSMITTAL WHERE BENEFIT OF PRIOR U.S. APPLICATION(S) CLAIMED.

10. Fee Calculation (37 C.F.R. 1.16)

A. ☒ Regular application

CLAIMS AS FILED			
Number Filed	Number Extra	Rate	Basic Fee
			37 C.F.R. 1.16(a)
			\$690.00
Total Claims			
[37 CFR 1.16(c)] 12-20 = 0	0	x \$18.00	0
Independent Claims [37 CFR 1.16(b)]			
7-3 = 4	4	x \$78.00	312.00
Multiple dependent claim(s), if any			
[37 CFR 1.16(d)]	0	+ \$260.00	0

☐ Amendment cancelling extra claims is enclosed.

☐ Amendment deleting multiple-dependencies is enclosed.

☐ Fee for extra claims is not being paid at this time.

NOTE: If the fees for extra claims are not paid on filing they must be paid or the claims cancelled by amendment, prior to the expiration of the time period set for response by the Patent and Trademark Office in any notice of fee deficiency. 37 CFR 1.16(d).

Filing Fee Calculation

\$1002.00

- B. ☐ Design application
[\$310.00—37 CFR 1.16(f)]

Filing Fee Calculation \$

- C. ☐ Plant application
[\$480.00—37 CFR 1.16(g)]

Filing Fee Calculation \$

11. Small Entity Statement(s)

- ☐ Verified Statement(s) that this is a filing by a small entity under 37 CFR 1.9 and 1.27 is (are) attached.

WARNING: *Status as a small entity in one application or patent does not affect any other application or patent, including applications or patents which are directly or indirectly dependent upon the application or patent in which the status has been established. A nonprovisional application claiming benefit under 35 U.S.C. 119(e), 120, 121 or 365(c) of a prior application may rely on a verified statement filed in the prior application if the nonprovisional application includes a reference to a verified statement in the prior application or includes a copy of the verified statement filed in the prior application if status as a small entity is still proper and desired " 37 C.F.R. § 1.28(a).

(complete the following, if applicable)

- ☐ Status as a small entity was claimed in prior application.
_____/_____, was filed on _____, from which
benefit is being claimed for this application under:

35 U.S.C. ☐ 119(e),

☐ 120,

☐ 121,

☐ 365(c),

and which status as a small entity is still proper and desired.

- ☐ A copy of the verified statement in the prior application is included.

Filing Fee Calculation (50% of A, B or C above)

\$ _____

NOTE: Any excess of the full fee paid will be refunded if a verified statement and a refund request are filed within 2 months of the date of timely payment of a full fee. The two-month period is not extendible under § 1.136, 37 CFR 1.28(a).

12. Request for International-Type Search [37 C.F.R. 1.104(d)]

(complete, if applicable)

- ☐ Please prepare an international-type search report for this application at the time when national examination on the merits takes place.

13. Fee Payment Being Made at This Time

☐ Not Enclosed

☐ No filing fee is to be paid at this time.
(This and the surcharge required by 37 C.F.R. 1.16(e) can be paid subsequently).

☒ Enclosed

☒ Filing fee \$1002.00

☐ Recording assignment _____
[\$40.00; 37 C.F.R. 1.21(h)]
(See attached "COVER SHEET FOR ASSIGNMENT
ACCOMPANYING NEW APPLICATION"). _____

☐ Petition fee for filing by other than all the inventors or
person on behalf of the inventor where inventor refused
to sign or cannot be reached _____
[\$130.00; 37 C.F.R. 1.47 and 1.17(h)]

☐ For processing an application with a specification
in a non-English language _____
[\$130.00; 37 C.F.R. 1.52(d) and 1.17(k)]

☐ Processing and retention fee _____
[\$130.00; 37 C.F.R. 1.53(d) and 1.21(l)]

☐ Fee for international-type search report _____
[\$40.00; 37 C.F.R. 1.21(e)]

NOTE: 37 CFR 1.21(l) establishes a fee for processing and retaining any application that is abandoned for failing to complete the application pursuant to 37 CFR 1.53(d) and this, as well as the changes to 37 CFR 1.53 and 1.78, indicates that in order to obtain the benefit of a prior U.S. application, either the basic filing fee must be paid, or the processing and retention fee of § 1.21(l) must be paid, within 1 year from notification under § 53(d).

Total fees enclosed \$1002.00

14. Method of Payment of Fees

☐ Check in the amount of \$ _____

☒ Charge Account No. 50-0270 in the amount of \$1002.00

Two duplicates of this transmittal are attached.

NOTE: Fees should be itemized in such a manner that it is clear for which purpose the fees are paid. 37 CFR 1.22(b).

0044630 " 9464560

15. Authorization to Charge Additional Fees

WARNING: If no fees are to be paid on filing, the following items should not be completed.

WARNING: Accurately count claims, especially multiple dependent claims, to avoid unexpected high charges, if extra claim charges are authorized

- ☒ The Commissioner is hereby authorized to charge the following additional fees by this paper and during the entire pendency of this application to Account No. 50-0270.

☒ 37 C.F.R. 1.16(a), (f) or (g) (filing fees)

☒ 37 C.F.R. 1.16(b), (c) and (d) (presentation of extra claims)

NOTE: *Because additional fee for excess or multiple dependent claims not paid on filing or on later presentation must only be paid or these claims cancelled by amendment prior to the expiration of the time period set for response by the PTO in any notice of fee deficiency [37 CFR 1.16(d)], it might be best not to authorize the PTO to charge additional claim fees, except possibly when dealing with amendments after final action.*

☒ 37 C.F.R. 1.16(e) (surcharge for filing the basic filing fee and/or declaration on a date later than the filing date of the application)

☒ 37 C.F.R. 1.17 (application processing fees)

WARNING: While 37 CFR 1.17(a), (b), (c) and (d) deal with extensions of time under § 1.136(a), this authorization should be made only with the knowledge that "Submission of the appropriate extension fee under 37 C.F.R. 1.136(a) is to no avail unless a request or petition for extension is filed." (Emphasis added). Notice of November 5, 1985 (1060 O.G. 27).

☐ 37 C.F.R. 1.18 (issue fee at or before mailing of Notice of Allowance, pursuant to 37 C.F.R. 1.311(b))

NOTE: *Where an authorization to charge the issue fee to a deposit account has been filed before the mailing of a Notice of Allowance, the issue fee will be automatically charged to the deposit account at the time of mailing the notice of allowance. 37 CFR 1.311(b).*

NOTE: *37 CFR 1.28(b) requires "Notification of any change in loss of entitlement to small entity status must be filed in the application...prior to paying, or at the time of paying,...issue fee." From the wording of 37 CFR 1.28(b): (a) notification of change of status must be made even if the fee is paid as "other than a small entity" and (b) no notification is required if the change is to another small entity.*

16. Instructions as to Overpayment

☒ Credit Account No. 50-0270.

☐ Refund

Reg. No. 39,368

Tel. No. (972) 894-6173



Signature of Attorney

Steven A. Shaw
(type or print name of attorney)

Nokia Inc.

6000 Connection Drive 1-4-755
(P.O. Address)

Irving, TX 75039

☒ **Incorporation by reference of added pages**

[check the following item if the application in this transmittal claims the benefit of prior U.S. application(s) (including an International Application entering the U.S. stage as a continuation, divisional or C-I-P application) and complete and attach the ADDED PAGES FOR NEW APPLICATION TRANSMITTAL WHERE BENEFIT OF PRIOR U.S. APPLICATION(S) CLAIMED.]

- ☒ Plus Added Pages for New Application Transmittal Where Benefit of Prior U.S. Application(s) Claimed

Number of pages added 1

- ☐ Plus Added Pages for Paper Referred to in Item 4 Above

Number of pages added _____

- ☐ Plus "Assignment Cover Letter Accompanying New Application"

Number of pages added _____

☐ **Statement Where No Further Pages Added**

(if no further pages form a part of this Transmittal, then end this transmittal with this page and check the following item)

- ☐ This transmittal ends with this page.

Attorney Docket No. NC13977

PATENT

ADDED PAGES FOR APPLICATION TRANSMITTAL WHERE BENEFIT OF
PRIOR U.S. APPLICATION(S) CLAIMED

35 U.S.C. 119(e)

This application claims the benefit of U.S. Provisional Application(s)
No(s).:

APPLICATION NO(S).

FILING DATE

60/150,732

August 25, 1999

004200" 94091950

KEY DISTRIBUTION FOR ENCRYPTED BROADCAST DATA USING MINIMAL SYSTEM BANDWIDTH

RELATED APPLICATIONS

Applicant claims benefit of earlier filed United States Provisional
5 Application number 60/150,732 filed on August 25, 1999, on behalf of Scott
Probasco entitled "KEY DISTRIBUTION FOR ENCRYPTED BROADCAST
DATA USING MINIMAL SYSTEM BANDWIDTH."

BACKGROUND OF THE INVENTION

10 This invention relates generally to communication networks and, more
particularly a key distribution system for a broadcast network.

Modern communications systems may include a type of delivery
service known as "broadcast" addressing wherein a single source node
broadcasts information or messages (i.e. data) to multiple receiver nodes by
sending a single instance of the data or message. This type of service uses
15 efficient addressing mechanisms to deliver a single delivery instance of the
data to multiple receiver nodes using minimal system resources or bandwidth.
Broadcast addressing is achieved by using a special code in the address field
of message (or data packet). The originator, or source, of the data may
desire to use this efficient broadcast addressing mechanism to deliver the
20 data, but still be able to control access to the data such that only authorized
receiver nodes may interpret the data. A common method to control access
to data is to encrypt the data at its source. Only receiver nodes possessing
the correct key to decrypt the data are able to interpret the data, and access
is thus controlled.

25 Some broadcast systems also support a subset transmission mode
referred to as "multicast" addressing wherein the transmission is to a subset
of the machines on a network.

Fig. 1 shows a typical communication system. Network 100 may comprise Broadcast Server(s) 110 as a single source node, Database 115 coupled to Broadcast Server(s) 110, Internet 120 to which broadcast service is coupled. Network 100 also comprise various receiver nodes such as:

5 Mobile Switching Center (MSC) 130 which is coupled to a plurality of Base Stations 150, each Base Station 150 may be in wireless communication with a plurality of Mobile Stations 160. A plurality of MSCs and their associated Base Stations made form a host cellular network. Other nodes may include Network Access Point 190, which may be a server, gateway, bridge, or router

10 providing access to the Internet for various devices 195. Another node to Network 100 may be a Public Service Telephone Network (PSTN) 170 which may provide an access point for various telephonic devices 180.

In a dynamic environment, a problem exists to efficiently maintain the list of authorized receiver nodes (those nodes having the correct key). Of

15 particular interest is the ability to update the list of authorized receiver nodes (add or delete members) without impacting the entire population of authorized receiver nodes.

For example, a news delivery service might wish to deliver news headlines on a periodic basis to authorized receiver nodes who have

20 negotiated a subscription. In this case, the news delivery service (or source of the data) would encrypt the data so that interpretation of the data is limited to those receiver nodes who have negotiated a subscription (and therefore have been provided with the key to the data). When additional receiver nodes acquire a subscription, these nodes must be provided access to the

25 data (or decryption key) without disturbing the access of other receiver nodes. Also, when a receiver nodes' subscription is no longer valid, the capability must exist to discontinue the receiver nodes' access to the data (or decryption key) without disturbing the access of other receiver nodes.

Thus, there is a need to provide a bandwidth efficient distribution

30 technique for a source of material to manage the broadcast of said material over a network to multiple users in a secure manner.

SUMMARY OF THE INVENTION

This invention provides a bandwidth-efficient mechanism whereby the source or originating node(s) (the invention supports multiple source nodes, each creating single or multiple broadcast message(s)) may utilize broadcast
5 addressing service to efficiently reach multiple receiver nodes and still control which receiver node(s) may access the broadcast data or message. This method is realized by a novel and efficient key distribution technique

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is an illustration of a typical broadcast network.

10 Fig. 2 is an illustration of a typical protocol stack.

Fig. 3 is an illustration of a Wireless Application Protocol (WAP) stack.

Fig. 4 is a flowchart showing the steps of a processing keys in accordance with embodiments of the invention.

15 Fig. 5 is a flowchart showing the steps of requesting keys in accordance with embodiments of the invention.

DETAILED DESCRIPTION

Modern communications systems may be described in an abstract manner by a series of layers defining protocol hierarchies or stacks. Network architectures are organized in layers in order to reduce design complexity.

5 Each layer provides services to the layer above it, thus protecting the above layers from the details of actual implementation of the provided services. A layer on one machine communicates with the corresponding layer on another machine. Each layer has a plurality of protocols which are the rules and methods of communication. Herein the applicant defines the term plurality to
10 mean one or more.

One example of a network architecture organized as a stack is the Open Systems Interconnection (OSI) Reference Model. The most common example of a protocol stack is the TCP/IP Reference Model. A treatment of the TCP/IP model may be found in *TCP/IP Illustrated, Volume 1, 2, 3* by W.
15 Richard Stevens (Addison-Wesley) incorporated herein by reference. Other reference models include Wireless Application Protocol (WAP)—which will be discussed below--and Broadband Integrated Services Digital Network (B-ISDN).

Fig. 2 is an illustration of a typical "bottom up" reference model
20 comprising Physical Layer (Layer 1) 210, Link Layer (Layer 2) 220, Network Layer (Layer 3) 230, Transport Layer (Layer 4) 240, and a plurality of application specific layers above the other layers (Layer 4+) 250, 260...

Physical Layer 210 deals with the electrical, mechanical, procedural
25 interfaces between the physical transmission medium, which lies below the physical layer, and the layers above Physical Layer.

Link Layer 220 organizes the data coming from Physical Layer 210. Link Layer 220 may break the data stream into data frames by creating frame boundaries. This is done by attaching special bit patterns to the beginning and ending of the frame. It is in Link Layer 220 where broadcast networks

must deal with controlling access to the shared channel. This is dealt with by Medium Access Sublayer 225.

Network Layer 230 controls the routing of the messages or data packets from a source node to a destination node and controlling the operation of the subnet. A protocol in the network layer of the TCP/IP model in Internet Protocol (IP).

Transport Layer 240, among other duties, determines the type of service. In the case of the present invention, the service is a broadcast type or a multicast type service. Transport Layer 240 accepts messages or data from the upper layer, splits the data into smaller units, if needed, and sends them to Network Layer 230. Two protocols in this layer in the TCP/IP model are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).

Application Layers 250, 260...may be various protocols that may be needed such as File Transfer Program (FTP), HyperText Transfer Protocol (HTTP), NNTP—a protocol for moving news articles, directory lookup, e-mail and the like.

Various embodiments of the invention allow for encryption of the source data at the application layer, transport layer, and network layer.

The destination nodes of the broadcast network may also comprise wireless devices known as mobile stations. A reference model based on the TCP/IP model called Wireless Application Protocol (WAP) was developed to address the screen size and bandwidth limitations of these mobile stations. A full-treatment of Wireless Application Protocol (WAP) may be found at <http://www.wapforum.org>.

Fig. 3 is an illustration of the network architecture for WAP. WAP Protocol Stack 300 comprises Transport Layer (WDP) 310, Security Layer (WTLS) 320, Transaction Layer (WTP) 330, Session Layer (WSP) 340, Application Layer (WAE) 350, and other services and applications 360. WAP Protocol Stack also provides Bearer Services Layer 370 for services such as

Short Message Service (SMS), Code Division Multiple Access (CDMA), Cellular Digital Packet Data (CDPD) and the like.

The names provided for the layers in the WAP architecture is: Wireless Datagram Protocol (WDP), Wireless Transport Security (WTLS), Wireless Transaction Protocol (WTP), Wireless Session Protocol (WSP), Wireless Application Environment (WAE).

The various reference models are provided as exemplars only. The embodiments of the present invention may be utilized in other network architecture. Therefore, the layer names below do not refer to specific architectures unless noted otherwise.

Application Layer

In a first embodiment of the invention, a method in accordance with the invention is applied at the "application" or "Teleservice" layer of a protocol stack in a communications system. A source node, such as Broadcast Server(s) 110 described above in Fig. 1, encrypts the message(s) to be broadcast with an encryption key. A single encryption key may be used for all messages, or different encryption keys may be used for different groups of messages or even a unique encryption key used for each unique message. If any additional network entity is to have authority to grant access to the encrypted messages, each encryption key(s) is sent, by any secure means, to this authorized entity. An example of such an authorized entity is host cellular network(s) as was described in Fig. 1 above. At the source node, each encryption key is "hashed" through techniques known by those skill in the art, such as a common one-way or trap-door function, to provide a hash representation of the encryption key. A trap-door function is one in which any party can compute the function, but only the intended receiving can compute the inverse function. Each encrypted message and the hash of the its encryption key are delivered from the source node to multiple users via broadcast delivery service.

Any of the multiple receiving nodes may process the received message in the method described as follows referring to Fig. 4 and Fig.1. The receiving node may be end-user equipment supporting encryption such as Mobile Station 160, computing terminals 195 or telephonic devices such as fax, telephone and the like 180 of Fig. 1. The receiving node may also be a node away from the end-user such as MSC 130, Base Station 150, Access Points 190 and 170 of Fig. 1.

Referring now to Fig. 4. The method starts at step 4000 when receiving node receives data. At step 4100, the receiving node parses the broadcast data to identify an encrypted message and its' hashed key. The receiving node determines if it has a key or a non-null key (step 4200). If the receiving node has no key(s) or possesses a NULL key to decrypt the message(s), the receiving node may request a key as will be described below and as is shown in Fig. 5 (4210). If the receiving node has one or more non-NULL keys, the receiving node examines each key it possesses in turn to determine a key match. The method continues with the examination steps. At step 4300, the receiving node hashes one of its own key (using the same one-way or trap-door function as the source node) and compares the result with the received hashed key (step 4400). If there is not a match 4500 and the receiving node has additional keys 4410 the process returns to step 4300 and repeat steps 4300 to 4410 until the receiving node has no compared keys remaining. If none of the key hashes match, the receiving node does not possess a valid key; the receiving node may request a key using method described below and shown in Fig. 5 (step 4210). If one of the key hashes do match, the receiving node does possess the proper key and may decrypt the message(s) (step 4600). The above is to be used as exemplar only variations and modifications may become known to those skilled in the art after reading the specification. Such variations and modifications are deemed to be within the spirit and scope of the invention.

For example, the receiving node may hash all its keys at step 4300 and then compare its hashed keys with the received key.

Referring to Fig. 5, when the receiving node wishes to request a key (either doesn't have a key or doesn't have the correct key), a request may be sent to each network entity which has granted a subscription to the receiving node (step 5100). This may include a key request directly to the source node.

5 The request may ask for all keys the subscription is entitled to or specific keys depending upon the subscription (e.g. all updated keys, all keys issued or changed after a specific date and time, or a specific key). At step 5200, the network entity receives the request. At step 5300, a decision to grant the request or deny the request is made. At step 5300, more information may be
10 required 5350, if the subscribed network entity does not recognize the requestor. Therefore, the process flows to step 5600 to uses processes known in the art to authenticate that the request is from an authorized receiver node before determining whether to grant or deny the request. If the request is granted, the network entity may send the key(s) to the receiver
15 node by any secure means (step 5400). If the request is denied, the network entity may notify the requesting node (step 5500).

At any time, a network entity with authority over the subscription may desire to add receiver nodes to the list of authorized recipients, or augment the subscription of a receiver node. This is accomplished by sending the new
20 key(s) to the receiver node. In this instance, the network entity would send an unsolicited key update message(s) to provide the receiver node with the appropriate key(s) for the subscription. At any time, a network entity with authority over the subscription may desire to remove a receiver node from the list of authorized receivers. This is accomplished by updating the receiver
25 node with a new key value (set to a known "NULL" value). In this instance, the network entity would send an unsolicited key update message(s) to either replace or amend the receiver node key list for the specific subscription with the contents of the message(s). Compliant receiver nodes will replace or amend the key list according to the update message(s).

30 The complexity of the above method increases as the number of encryption keys increases. For each encrypted message the receiving node

processes, the receiving node must compare the hash of each encryption key in its possession to the received hash to determine if the received message can be decrypted. Another embodiment of the invention may be realized by introducing the concept of "categories" of messages.

5 A source node encrypts the message(s) to be broadcast with an encryption key. A single encryption key may be used for all messages, or different encryption keys may be used for different groups of messages or even a unique encryption key used for each unique message. Each unique encryption key is associated with a category. More than one encryption key
10 may be associated with the same category. If any additional network entity is to have authority to grant access to the encrypted messages, each encryption key(s) and associated category are sent, by any secure means, to this authorized entity--for example a host cellular network(s) as shown in Fig. 1. At the source node, each encryption key is "hashed" through a common
15 one-way or trap-door function to provide a hash representation of the encryption key. Each encrypted message, the hash of the its encryption key, and the associated category of the encryption key are delivered from the source node to multiple users via broadcast delivery service.

Any of the multiple receiving nodes may process the received
20 message using the method shown in Fig. 4 with the modification of the key(s) being associated with a category. Said modified method is as follows. The receiving node parses the broadcast data to identify an encrypted message, its hashed key, and the associated category. If the receiving node has no key(s) or possesses a NULL key associated with the category, the receiving
25 node may request a key which is associated with the category as will be described below in association with Fig. 5. If the receiving node has one or more non-NULL keys associated with the category, the receiving node may examine each key it possesses for that category in the following way to determine a key match: the receiving node hashes its own key(s) associated
30 with the category (using the same one-way or trap-door function as the source node) and compares the result(s) with the received hashed key. If

none of the key hashes match, then the receiving node does not possess a valid key to decrypt the message(s). Therefore, the receiving node may request a key in a method as described below in association with Fig. 5. If one of the key hashes do match, the receiving node does possess the proper key and may decrypt the message(s).

Variations and modifications may become known to those skilled in the art after reading the specification. For instance, the receiving node may hash all its keys and then compare its hashed keys with the received key to determine if the receiving node has any keys associated with the hashed category.

The following method to request a key is similar to the description of Fig. 5 with the modification that the key(s) are associated with a category. When the receiving node wishes to request a key (either doesn't have a key or doesn't have the correct key), a request may be sent to any network entity which has authority over a subscription to the receiving node. This may include a key request directly to the source node. The request may ask for all keys the subscription is entitled to or specific keys depending upon the subscription (e.g. all keys associated with a specific category, all updated keys, all keys issued or changed after a specific date and time, or a specific key). The network entity receives the request, and may grant the request, deny the request, or initiate any processes to authenticate that the request is from an authorized receiver node before determining whether to grant or deny the request. If the request is granted, the network entity may send the key(s) and associated category to the receiver node by any secure means. If the request is denied, the network entity may notify the requesting node.

At any time, a network entity with authority over the subscription may desire to add receiver nodes to the list of authorized recipients, or augment the subscription of a receiver node. This is accomplished by sending the new key(s) and associated category to the receiver node. In this instance, the network entity would send an unsolicited key update message(s) to provide the receiver node with the appropriate key(s) and associated category for the

subscription. At any time, a network entity with authority over the subscription may desire to remove a receiver node from the list of authorized receivers. This is accomplished by updating the receiver node with a new key value (set to a known "NULL" value) and its' associated category. In this instance, the network entity would send an unsolicited key update message(s) to either replace or amend the receiver node key and its' associated category list for the specific subscription with the contents of the message(s). Compliant receiver nodes will replace or amend the key and associated category list according to the update message(s).

Note that the Basic Method and Optimized Method may be combined in a single implementation. In this implementation, the Optimized Method is used, and any encryption keys which are not explicitly associated with a category implicitly belong to the same, "unlisted" or "unspecified" category. The Basic Method is seen to be a subset of the Optimized Method, where all encryption keys belong to a single, implicit category.

Transport Layer Method

Another embodiment of the invention is applied at the Transport Layer in a communications system. An application or "Teleservice," in a source node, defines an application message(s) or data unit(s) to be broadcast. The application message(s) contains more data than the transport path to the destination communication system can transmit in a single unit. This transport path may comprise of one or more logical blocks, not necessarily co-located, and may or may not include components in more than one data communications systems. In this instance, the application message(s) must be segmented by the communications system at the source node and then reassembled at the receiver node before the application message(s) are delivered to the application. A Teleservice Segmentation and Reassembly (TSAR) function may provide encryption of each segment of data as an implementation option.

For an efficient implementation of a Transport Layer or TSAR function, the overhead information of the Transport Layer or TSAR function is

described and transported once for an entire Teleservice Message as header information from the Transport Layer or TSAR function. Indication of encryption and the Hash of the encryption key may be included in the Transport Layer or TSAR header information. In this instance, both the

5 Application Layer Method Basic Method and Application Layer Method
Network Layer Method

An additional embodiment of the invention may be applied at the Network Layer in a communications system. One node of communications network, e.g. a Gateway or Switch function, receives incoming data that is
10 addressed to multiple receiver nodes in the communications network via broadcast addressing. For a variety of reasons (subscription, liability, content), the controlling entity of the communications system may wish to restrict access to this information to authorized receiver nodes, independent of the restrictions implemented by the source(s) of the incoming data.

15 At the Network Layer, typical implementations of a communications system use a "wrapper" data element to contain "higher layer" data and Network Layer addressing and control data (e.g. an R-Data message or SMDPP message in certain communications systems), and thus delivers this "wrapper" data element intact to receiver nodes. In this instance, both the
20 embodiments of the invention implemented at the Application Layer as described above, may be applied at the Network Layer to restrict access to the "higher layer" data to a subset of authorized receiver nodes when broadcast addressing is used.

Alternative to the Hash or Trap-door Function

25 In the above embodiments, the encryption key itself is transformed by a Hash or Trap-door function so that this Hash of the encryption key may be transported over a potentially non-secure communications path. The "strength" of the protection provided is a function of the length of the key and strength of the Hash function. The longer the key the stronger the protection.
30 The more mathematically strong the Hash function, the stronger the

protection. This additional strength requires additional implementation complexity in the form of bandwidth to transport the Hash of the encryption key and additional computing power to compute the Hash of the key. The choice of strength versus complexity is an implementation choice.

5 A less complex method can be utilized in place of the encryption key Hash. In this method, the source node selects an encryption key(s) according to any method. This encryption key(s) is used to encrypt the source message(s). The source node sends the encryption key and an associated "tag" to any network entity with authority over the subscription, by any secure
10 means. The encrypted message and its' associated tag are delivered from the source node to multiple users via broadcast delivery service.

 This alternative encryption key identification scheme can be optimized by subdividing the tag field to include a source node identifier as well as an encryption key tag field. In this way, large numbers of source nodes can exist
15 in the same communications system without coordinating the assignment of tag identifiers. This alternative is seen to be applicable to all methods discussed above.

 The above embodiments may be augmented to provided additional functionality with reduced system overhead by including with the encryption
20 key a "timer" value which indicates how many time-units the key may be used before compliant systems replace the key with a known "NULL" value. A particular embodiment of this method would allow temporary additions to the list of authorized receiver nodes for a predetermined time period with zero system resources or overhead required to remove the receiver node from the
25 list after a trial or introductory period.

 It is seen that the invention supports delivery of encrypted broadcast messages at various layers of the protocol stack. A basic method to provide the encryption key(s) to each member of the authorized receiver node list is to send the encryption key(s) to each authorized receiver node on the list in a
30 point to point addressed secure message. While individual receiver nodes may be added to the list without undue burden on system throughput and

capacity, removing a receiver node from the list may only be accomplished by sending a point to point addressed secure message with the new encryption key(s) to every remaining authorized receiver node on the list. This is seen to be an inefficient and poor use of system capacity and bandwidth. This invention describes methods which allows the host communication system or source node (any network entity with authority over the subscription) to add or remove individual receiver nodes from the list of authorized receiver nodes with minimal impact on system resources and capacity. These methods provide a fully functional key distribution system for broadcast addressing with minimal system overhead requirements, has the flexibility to be applied to any communications system, at multiple layers of the protocol stack.

Although described in the context of particular embodiments, it will be apparent to those skilled in the art that a number of modifications to these teachings may occur. Thus, while the invention has been particularly shown and described with respect to one or more preferred embodiments thereof, it will be understood by those skilled in the art that certain modifications or changes, in form and shape, may be made therein without departing from the scope and spirit of the invention as set forth above and claimed hereafter. The applicant herein defines "plurality" to be one of more.

CLAIMS

What is claimed is:

- 1 1. A method for sending secure messages in a broadcast network
2 comprising the steps of:
3 encrypting data with a key;
4 hashing said key;
5 combining said encrypted data and said key in a broadcast
6 message; and
7 transmitting said broadcast message to a plurality of receiving
8 nodes.
- 1 2. The method of claim 1 wherein the key is a plurality of different keys
2 and said steps of combining and transmitting comprises:
3 combining said encrypted data with each one of said plurality of
4 different keys in a plurality of broadcast messages; and
5 transmitting one of the plurality of broadcast messages to a
6 subset of said plurality of receiving nodes.
- 1 3. The method of claim 2 wherein each one of said plurality of different
2 keys are associated with a category.

- 1 4. A method for decrypting a message received over a broadcast
2 network comprising the steps of:
- 3 receiving data comprising an encrypted message and a hashed
4 key at a node in said broadcast network, wherein said node comprises
5 means for storing data;
- 6 parsing said data to derive said encrypted message and said
7 hashed key;
- 8 comparing said received hashed key with a plurality of keys
9 stored in said means for storing data in said node and to select a key
10 matching said received hashed key; and
- 11 decrypting said encrypted message with said matching key if a
12 match was found.
- 1 5. The method of claim 4 further comprising the step of requesting a key
2 from a network entity.
- 1 6. In a communications network having a plurality of network entities, a
2 first one of the network entities comprising:
- 3 a means encrypting data with a key;
- 4 a means for hashing said key;
- 5 a means for combining said encrypted data and said key in a
6 broadcast message; and
- 7 a means for transmitting said broadcast message to a plurality of
8 receiving nodes.
- 1 7. The network entity of claim 5 further comprising a means for
2 distributing hashed keys.

1 8. A computer-readable memory for directing a computer to function in a
2 particular manner when used by the computer, comprising:

3 a first portion to direct the computer to encrypt data with a key;

4 a second portion to direct computer to hash said key;

5 a third portion to direct computer to combine said encrypted data
6 with said key in a broadcast message; and

7 a fourth portion to direct computer to provide multiple
8 transmissions of said message.

1 9. A computer-readable memory for directing a computer to function in a
2 particular manner when used by the computer, comprising:

3 a first portion to direct the computer to receive data comprising an
4 encrypted message and a hashed key;

5 a second portion to direct computer to parse said data;

6 a third portion to direct computer to compare said received
7 hashed key with a plurality of keys and to select a key matching said
8 received hashed key; and

9 a fourth portion to direct computer decrypt said encrypted
10 message with said matching key if a match was found and send
11 request for key to a network entity if no matching key was found.

10. A computer data signal embodied in a carrier wave, comprising an encrypted message, a hashed key and instructions for:

parsing said data to derive said encrypted message and said hashed key;

comparing said received hashed key with a plurality of keys stored in said means for storing data in said node to select a key matching said received hashed key; and

decrypting said encrypted message with said matching key if a match was found and sending request for key to a network entity if no matching key was found.

11. A computer program product that enables a network entity distribute secure content in a network comprising:

computer readable code that instructs computer to:

encrypt data with a key;

hash said key;

combine said encrypted data and said key in a broadcast message;

transmit multiple transmissions of said broadcast message.

and

a tangible medium that stores the computer readable code.

12. The computer product of claim 11 wherein the tangible medium is selected from a group consisting of hard-disk, CD-ROM, DVD, floppy disk, flash memory and the like.

ABSTRACT

This invention provides a bandwidth-efficient mechanism whereby the source or originating node(s) (the invention supports multiple source nodes, each creating single or multiple broadcast message(s)) may utilize broadcast addressing service to efficiently reach multiple receiver nodes and still control which receiver node(s) may access the broadcast data or message. This method is realized by a novel and efficient key distribution technique.

004280" 92E54960

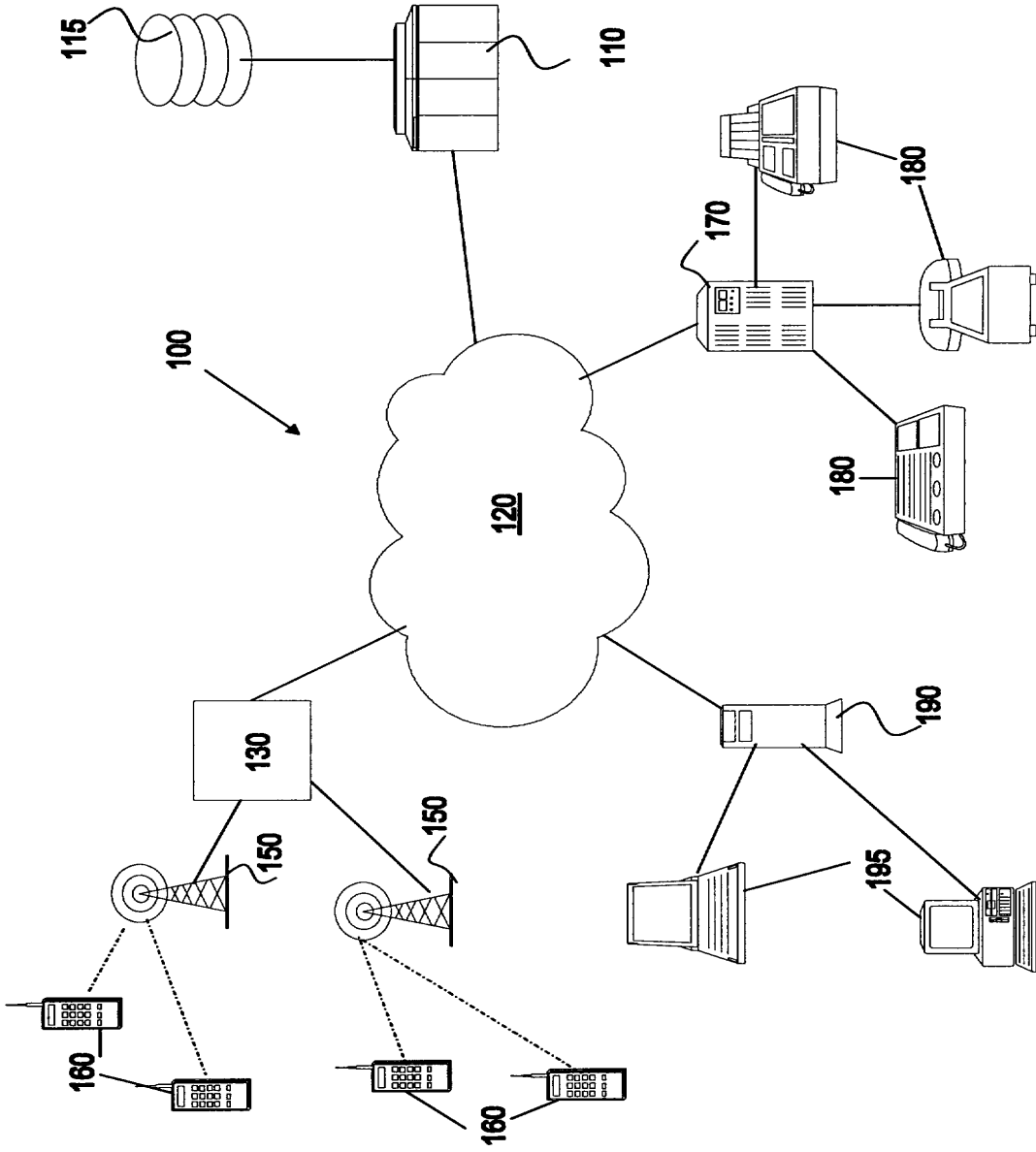


Fig. 1

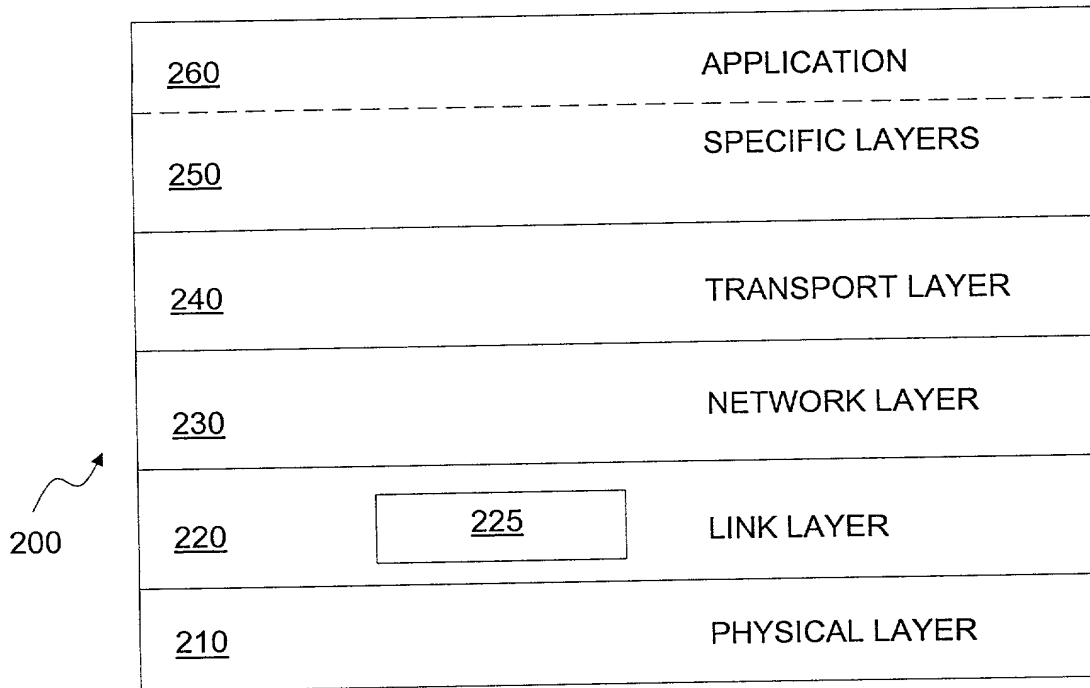


Fig. 2

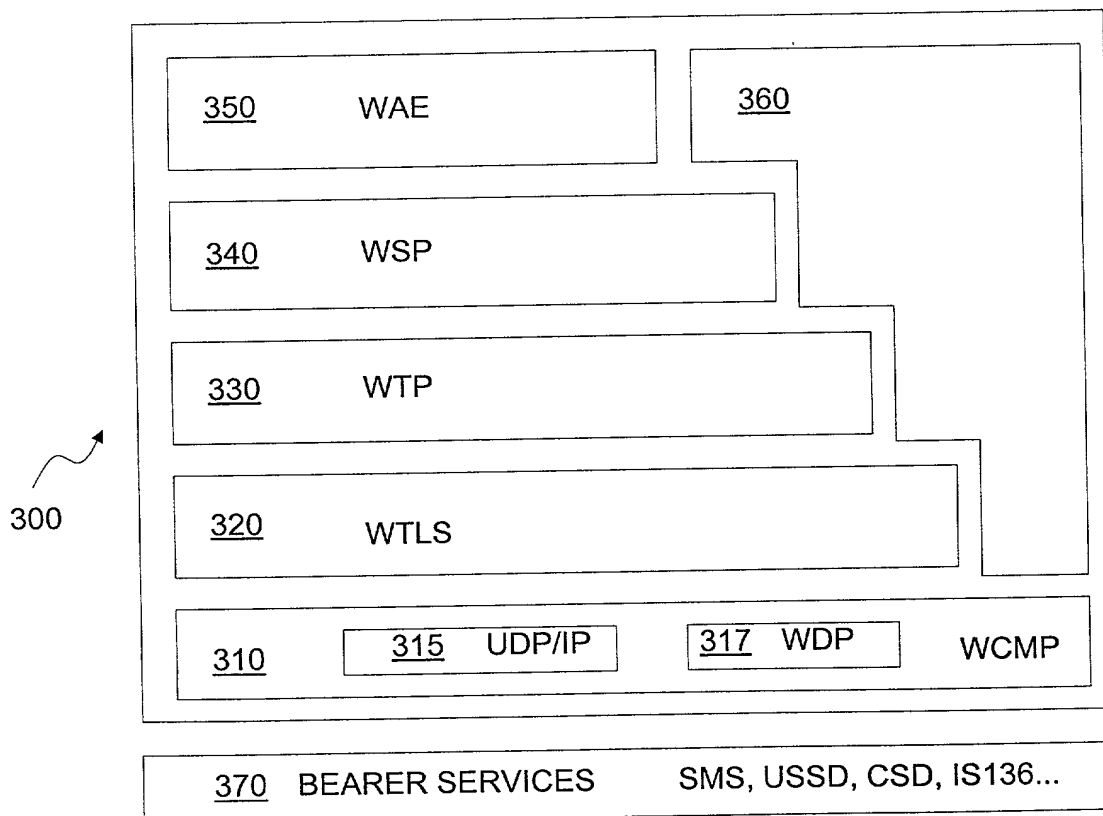


Fig. 3

004230" 94E84960

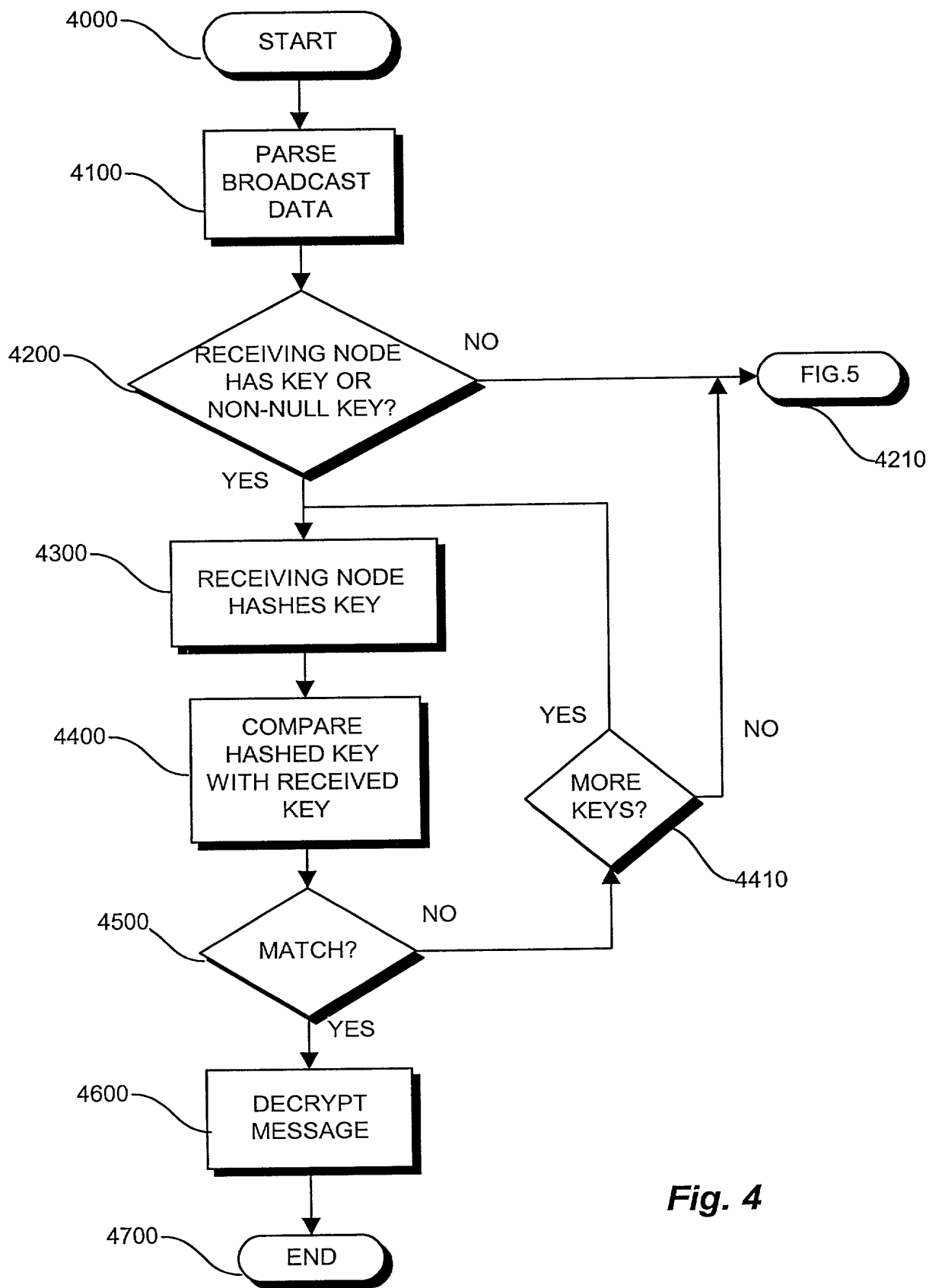


Fig. 4

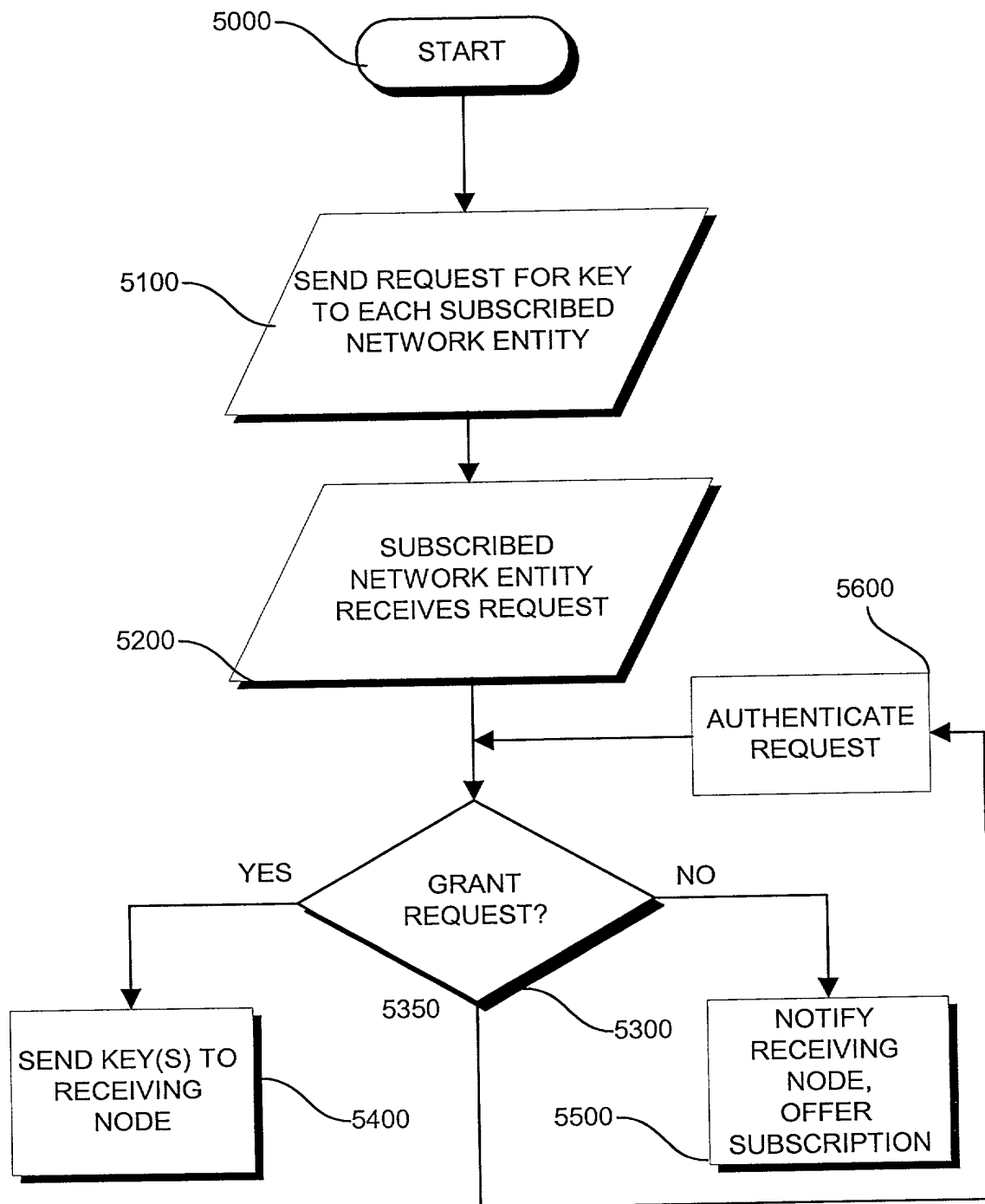


Fig. 5